REMARKS

By this Amendment, claims 1-19 are amended. Thus, claims 1-19 are active in the application. Reexamination and reconsideration of the application are respectfully requested.

The specification and abstract have been carefully reviewed and revised in order to correct grammatical and idiomatic errors in order to aid the Examiner in further consideration of the application. The amendments to the specification and abstract are incorporated in the attached substitute specification and abstract. No new matter has been added.

Also attached hereto is a marked-up version of the substitute specification and abstract illustrating the changes made to the original specification and abstract.

The Applicants thank the Examiner for acknowledging, in item 2 on page 2 of the Office Action, the Applicants' claim of foreign priority based on JP 2000-3844835. However, the Applicants note that the Examiner failed to acknowledge, in item 12 on the Office Action Summary form, the Applicants' claim of foreign priority and the receipt of the certified copy of the foreign priority document. Accordingly, the Applicants respectfully request the Examiner to acknowledge the Applicants' claim of foreign priority and the receipt of the certified copy of the foreign priority document.

In item 4 on page 2 of the Office Action, claims 1 and 3-19 were rejected under 35 U.S.C. § 102(e) as being anticipated by Dai (U.S. 6,081,598). This rejection is respectfully traversed for the following reasons.

The present invention provides a cryptocommunication system, method and program for ensuring the security of data transmission from third party attacks. The cryptocommunication system of the present invention includes a transmission apparatus and a reception apparatus. The cryptocommunication method and program of the present invention include a transmission operation and a reception operation.

Claims 1 and 18 recite the transmission apparatus of the present invention, and claims 15-17 recite the transmission operation of the present invention.

The transmission apparatus is recited in claims 1 and 18 as comprising first generation means for generating first additional information, first operation means for performing an invertible operation on the plaintext and the first additional information to generate connected information, and encrypting means for encrypting the connected information according to an encryption algorithm so as to generate the ciphertext.

The transmission operation is recited in claims 15-17 as comprising generating first additional information, performing an invertible operation on the plaintext and the first additional information to generate connected information, and encrypting the connected information according to an encryption algorithm so as to generate the ciphertext.

Dai discloses a cryptographic system which includes an encoder 22 (transmission apparatus) and a decoder 24 (reception apparatus). The encoder transforms a message M into ciphertext C and transmits the ciphertext C over a communications channel 26 (see Figure 1). Dai discloses that the message M is encrypted by using a value W, where $W = h_1(x)$ xor M (xor = exclusive OR function) (see Column 3, lines 58-67). "xor" is considered to correspond to an encryption algorithm.

If the Examiner considers that "$W = h_1(x)$ xor M" corresponds to the encrypting means of claims 1 and 18 or the encrypting operation of claims 15-17, then Dai cannot be interpreted as disclosing any operation or circuitry remotely resembling a first operation means for performing an invertible operation on the plaintext (M) and the first additional information to generate connected information, as recited in claims 1 and 18, or performing an invertible operation on the plaintext (M) and the first additional information to generate connected information, as recited in claims 15-17.

On the other hand, if the Examiner considers that "x" corresponds to the first additional information of claims 1 and 15-18, and that "$W = h_1(x)$ xor M" corresponds to the invertible operation performed in the transmission apparatus and operations of claims 1 and 15-18, where "W" would be the generated connected information, then Dai cannot be interpreted as disclosing any operation or circuitry remotely resembling encrypting means for encrypting the connected information according to an encryption algorithm so as to generate the ciphertext, as recited in claims 1 and 18, or encrypting the connected information according to an encryption algorithm so as to generate the ciphertext, as recited in claims 15-17.

In other words, Dai can only be reasonably interpreted as disclosing either the first operation means of claims 1 and 18 or the encrypting means of claims 18. Similarly, Dai can only be reasonably interpreted as disclosing either performing the invertible operation or encrypting the connected information, as recited in claims 15-17.

The Examiner is respectfully reminded that anticipation requires disclosing each and every limitation of a claim. Accordingly, Dai clearly does not anticipate claims 1 and 15-17 since Dai fails to disclose each and every limitation of claims 1 and 15-17.

Furthermore, one skilled in the art would not have been motivated to modify the system of Dai to provide for either the first operation means or method and program element of claims 1 and 15-18 or the encrypting means or method and program element of claims 1 and 15-18 to arrive at the inventions of claims 1 and 15-18.

Accordingly, claims 1 and 15-18 are clearly not anticipated or rendered obvious by Dai since Dai fails to disclose or suggest each and every limitation of claims 1 and 15-18.

Therefore, claims 1 and 15-18 are clearly allowable over Dai.

In item 8 on page 5 of the Office Action, claim 2 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Dai in view of Jones (U.S. 5,412,730). As demonstrated above, Dai clearly fails to disclose or suggest the first operation means and the encrypting means of claims 1 and 18, as well as the corresponding operations of the program and method of claims 15-17.

Jones also fails to disclose or suggest the first operation means and encrypting means of claims 1 and 18 as well as the corresponding operations of the program and method of claims 15-17.

Therefore, Jones fails to cure the deficiencies of Dai for failing to disclose or suggest each and every limitation of claims 1 and 15-18.

Accordingly, no obvious combination of Dai and Jones would result in the inventions of claims 1 and 15-18 since Dai and Jones, either individually or in combination, clearly fail to disclose or suggest each and every limitation of claims 1 and 15-18.

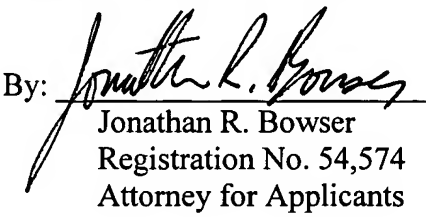
Furthermore, it is submitted that the clear distinctions discussed above are such that a person having ordinary skill in the art at the time the invention was made would not have been motivated to modify Dai and Jones in such as manner as to result in, or otherwise render obvious, the present invention as recited in claims 1 and 15-18. Therefore, it is submitted that the claims 1 and 15-18, as well as claims 2-14 and 19 which depend therefrom, are clearly allowable over the prior art as applied by the Examiner.

In view of the foregoing amendments and remarks, it is respectfully submitted that the present application is clearly in condition for allowance. An early notice thereof is respectfully solicited.

If, after reviewing this Amendment, the Examiner feels there are any issues remaining which must be resolved before the application can be passed to issue, the Examiner is respectfully requested to contact the undersigned by telephone in order to resolve such issues.

Respectfully submitted,

Masato YAMAMICHI et al.

By: 

Jonathan R. Bowser
Registration No. 54,574
Attorney for Applicants

JRB/nrj
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
September 1, 2005